MILLION EYES INSPECTOR: WINNING THE WAR ON COUNTERFEITING

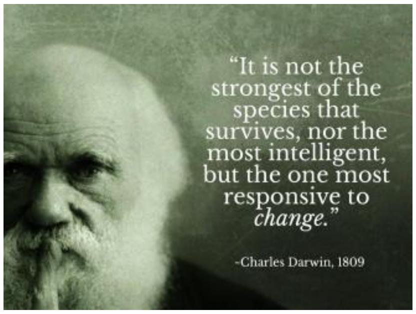
In a global economy where the stakes are high, the impact of counterfeiting to governments, companies, and public safety can be devastating. The need to protect against tax revenue loss to governments, to lessen the burden on law enforcement, to protect against intellectual property theft and revenue loss to brands, the loss of legitimate jobs, maintaining brand integrity and reputation, prevent possible injuries or loss of lives, and as in some cases, prevent the funding of criminal and terrorist activity[1], has never been more urgent.

Studies like the one conducted by Frontier Economics titled, "The Economic Costs of Counterfeiting and Piracy" report[2] have researched the threat landscape. Although precise data is difficult to obtain, they all arrive at consensus which suggests that counterfeiting deprives the global economy of over a trillion dollars a year - and project it to rise continually year over year.

As in warfare, and the fight against counterfeiting is war, defeating your opponent requires highly strategic defensive and offensive measures. Before you can begin developing a strategy however, it is imperative to understand some key principles; 1) Counterfeiters can and will imitate your brand, 2) no amount of enforcement, or any combination of technologies can prevent them from doing so, 3) no investments on their part is put into R&D, acquiring intellectual property, building brand recognition, developing supply chain partners, or marketing, 4) they are in the business to make money – yours, and 5) the Return on Investment is substantial.

Bullies do not attack the big and the strong. They seek out the smaller, weaker target to harass. Therefore, the deterrents you place in front of them must target the counterfeiter's core business model with the goal of deflecting their attention to the lower hanging fruits.

Arming your organization with strong and effective counterfeit prevention strategies and technologies is both an art and a science. In this article, we will offer a synopsis of various anti-counterfeit solutions, explore some of their benefits, analyze their vulnerabilities, and present a highly secured, highly effective solution.


"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to *change*."
-Charles Darwin, 1809

ANALOG SOLUTIONS

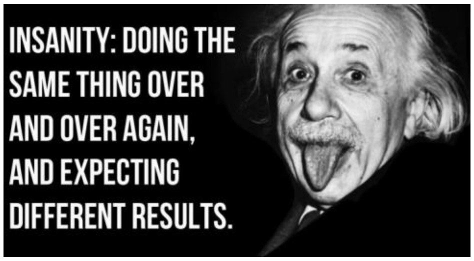
In the past, security technologies like security inks, security papers, holograms, chemical markers, DNA markers, nano-particles, and similar technologies were developed in hopes of thwarting counterfeiting. These technologies, categorized as analog security solutions, are generally limited to corporate inspectors, customs organizations, and/or supply chain partners. Some of them require the use special detection devices that are burdensome and costly, while others are subject to forensic testing in controlled laboratory environments. With the exception of holograms and perhaps security paper, which requires user training, analog technologies limit a client's ability to detect and respond to fraudulent activity by ignoring the greatest asset in the fight on counterfeiting – the consumer. Additionally, analog technologies are manufactured by a 3rd party and can be intercepted in route to the client, and in some instances, counterfeited themselves[3]. In a digital world, one needs to question whether analog security solutions are destined for the history books, or still play a functioning role.

Figure 1 Nepal has termed India's Rs. 2000 and the new Rs. 500 currency notes "unauthorised and illegal". Photo: K. Murali Kumar | Photo Credit: K. Murali Kumar

IN A DIGITAL WORLD, DATA IS THE NEW OIL

In more recent years, digital authentication technologies have gained acceptance as an alternative or supplement to analog solutions. Whereas analog technologies offer little in terms of business intelligence and ROI, digital authentication technologies such as 2D barcodes, RFID, NFC, and other data carriers can uniquely identify every product at the tertiary, secondary, and even primary packaging level. Unique identification technologies can help organizations to enable real-time supply chain monitoring and optimization, hasten recall efforts, and by enabling consumer engagement, vastly broaden a company's detection and marketing capabilities – just to name a few.

Digital authentication technologies, although varying from provider to provider, all share a few common elements. The first is a unique identifier such as a serial number, checksum, or hash function encapsulated within the data carrier. These data carriers are attached to the product (asset) and are scannable by inspectors with a smartphone or handheld device. The second, a centralized database or blockchain that 'securely' stores sensitive information (information asset) for confirming/denying and recording authentication requests. And lastly, an internet or SMS gateway for communication. It should also be noted that some companies offer solutions that authenticate a label on the device and does not require connectivity.



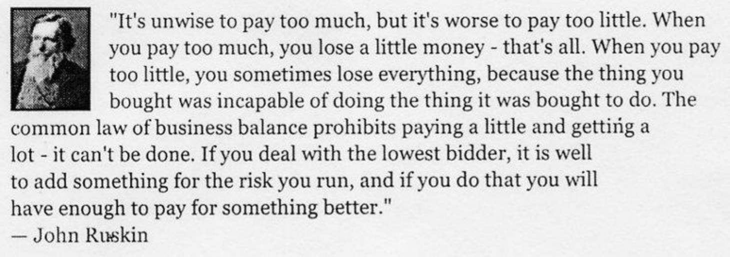
Unlike analog solutions, digital authentication technologies are far more complex in nature and requires a league of highly skilled professionals in the fields of technology, information management, network engineers, cryptographers, and cybersecurity to operate, maintain, and secure their infrastructure from attack.

When considering a digital authentication technology for protecting your intellectual property, it is important that you know what you're buying into. Many solution providers use clever jargon and make grandiose claims that their system is impenetrable, and therefore worthy of a purchase order. However, knowing that they often rely on 3rd party hardware and software, and that organizations such as Symantec, RSA, SAP, Oracle, Amazon, Google, Microsoft, Sony, Equifax, Target, Home Depot, JP Morgan, Anthem, Heartland Payment Systems, the US Office of Personnel Management, and that virtually every Fortune 1000 company and government has been hacked[4,5], should be of grave concern.

Mr. Tim Marsh, the Senior Director of Traceability, Provenance, Sustainability, and Blockchain once wrote[6] a hypothetical article in which he stated, "The database will be the "Holy Grail" quest for the sophisticated counterfeiters. By sophisticated I mean those interested in injecting large quantities of falsified medicines into a legitimate supply chain…If I'm a counterfeiter making wholly falsified product, again just hack into the databases, create false records of my serialized products and then offer it up for sale. As the product moves from trading partner to trading partner they simply add legitimacy to my original falsified database record."

SIDE NOTE: To gain a better perspective on these vulnerabilities, I highly recommend you read the following pragmatic articles on the subject[7,8].

For a counterfeiter, if the "juice is worth the squeeze," hiring bad actors to circumvent your digital authentication technology is highly plausible. The question is no longer an "if," it's a "when."



"It's unwise to pay too much, but it's worse to pay too little. When you pay too much, you lose a little money - that's all. When you pay too little, you sometimes lose everything, because the thing you bought was incapable of doing the thing it was bought to do. The common law of business balance prohibits paying a little and getting a lot - it can't be done. If you deal with the lowest bidder, it is well to add something for the risk you run, and if you do that you will have enough to pay for something better."
— John Ruskin

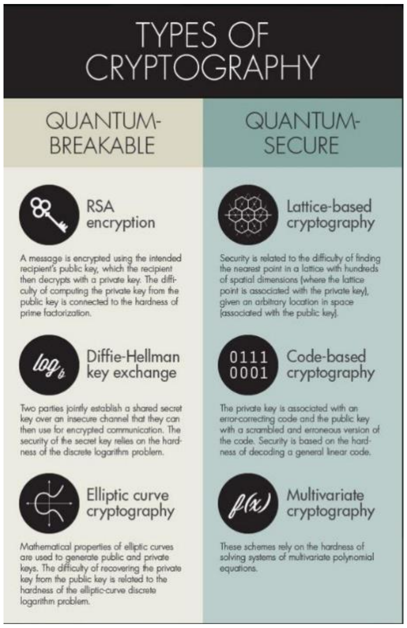
According to the Ponemon Institute's 2017 Cost of Data Breach Study[9], it took respondents 191 days on average to identify a breach and another 66 days to contain it. When sensitive or confidential information was involved, the average cost was $141 per record stolen. Although these figures decreased from 2016 (201 days to identify, 70 days to contain, and $158 per record), the average size of breaches in this study increased by 1.8%.

Add to the fact that 'the thing you bought was incapable of doing the thing it was bought to do,' any serialization impacted by such a breach can carry additional consequences such as massive recall efforts, loss of reputation, and in extreme circumstances, irreparable damage to a brand's reputation.

FACTS: serial numbers, hash functions, or encryption methods, like the ones used to generate a unique identifier have already been cracked,[10,11.12] and government, military, and corporate databases worldwide have been breached.[13]

Blockchain has recently seen a big push in the market thanks to cryptocurrencies. It is being touted by experts as a secure alternative to a centralized database system due to its claim of immutability – the inability to be modify a record after its been created.

Skeptics of Blockchain however seem to believe otherwise. For one, Blockchains run on the same servers with the same vulnerabilities as those that have been hacked. Those servers are not immune to malware, Trojan Horses, Zero Day or other attacks. And if they are immutable[14], as the claims lead us to believe, then experts in this space need to explain how the following attack[15] was carried out. With the invention of Quantum Computing, it will be very interesting to see how these technologies fair.



TYPES OF CRYPTOGRAPHY

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

QUANTUM-SECURE

Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).

Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate cryptography

These schemes rely on the hardness of solving systems of multivariate polynomial equations.

So if our databases and Blockchains are vulnerable to attack, how then do we solve this issue?

MICRO DATABASE LESS ENCAPSULATION (MDLE) – A CRYPTOCODEX, LTD. TECHNOLOGY

MDLE is an evolution in data security, storage, and authentication. Unlike other technologies that are limited to encapsulating non-essential information (serial number, etc.) into the data carrier, MDLE can encrypt the entire database record (relevant, sensitive information) and thus eliminate the need to maintain a vulnerable database or Blockchain – thus placing the information asset directly onto the asset[16].

THE BEST DEFENSE IS A GREAT OFFENSE – MDLE AND MILLION EYES INSPECTOR

"**Six degrees of separation** is the idea that all living things, and everything else in the world, are six or fewer steps away from each other so that a chain of "a friend of a friend" statements can be made to connect any two people in a maximum of six steps[17]."

Building upon this idea, Million Eyes Inspector is a strategic offensive system that combines modern technology (MDLE + smartphones), a firm understanding of human nature, social engineering theory, and fundamental knowledge and experience in information systems, cryptography, and cybersecurity. It empowers organizations with real-time access to secured data and reporting, provides for unparalleled detection capabilities of counterfeited or diverted products, connects your teams with supply chain partners, generates real-time logistical data, and most importantly, protects the consumers.

FACT – customs agencies are outnumbered and lack the resources to critically inspect every container entering the country.

Therefore, consumer engagement is strategically necessary, and has greater potential in radically reducing the burden on supply chain security professionals, law enforcement, and governments by substantially increasing the numbers of ‘eyes in the sky.’ This not only produces invaluable business intelligence, it connects the brand to the consumer and to a “friend of a friend,” that is unobtainable otherwise. This allows organizations to transform their marketing strategies in a way that is beyond imagination.[18,19]

For more information on how to protect your brand, feel free to email us at info@6dcp.com

[1] https://euipo.europa.eu/ohimportal/documents/11370/71142/Counterfeiting+%26%20terrorism/7c4a4abf-05ee-4269-87eb-c828a5dbe3c6

[2] https://cms.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016-Executive-Summary.pdf

[3] http://www.thehindu.com/news/national/counterfeiting-of-new-notes-worries-agencies/article17764449.ece

[4] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[5] https://securityaffairs.co/wordpress/45597/intelligence/china-hacked-us-defense-contractors.html

[6] https://www.linkedin.com/pulse/20140709193725-18691743-counterfeiter-targets-in-a-serialized-world/

[7] https://www.linkedin.com/pulse/you-weakest-links-goodbye-eddie-cohen/

[8] https://www.linkedin.com/pulse/serialization-youre-doing-wrong-eddie-cohen/

[9] https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

[10] https://pdfs.semanticscholar.org/54af/d43274e496d5e1b5e36faa21ce4e7dbf1340.pdf

[11] https://www.4armed.com/blog/hashcat-crack-md5-hashes/

[12] https://www.cut-the-knot.org/recurrence/guess.shtml#solution

[13] http://money.cnn.com/2011/10/27/technology/rsa_hack_widespread/index.htm

[14] https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/

[15] https://mashable.com/2018/04/05/verge-crypto-hack/

[16] http://www.6dcp.com/6DCP.pdf

[17] https://en.wikipedia.org/wiki/Six_degrees_of_separation

[18] http://www.6dcp.com/Coupon.jpg

[19] http://www.6dcp.com/ppt/6dma.pdf